AF

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Armano Montalvo

Serial No.: 09/688,609 Group Art Unit: 2131

Filed: October 13, 2000 Examiner: Sherkat, Arezoo

Title: SYSTEM FOR SECURE COMMUNICATIONS

Atty. Docket No.: PD-990304 (H 1168 PA)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief -Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

May 20, 2005 (Date of Deposit) Jo Anne Croskey Jo Anne Croskey (Signature)

APPEAL BRIEF

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

The following Appeal Brief is submitted pursuant to the Notice of Appeal filed May 3, 2005, in the above-identified application.

I Real Party in Interest

The real party in interest in this matter is The DirecTV Group, Inc of El Segundo, California which is 34 percent owned by Fox Entertainment Group, which is approximately 82 percent owned by The News Corporation, Limited.

II Related Appeals and Interferences

There are no other known appeals or interferences, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III Status of the Claims

Claims 1-10 are currently pending. Claims 1-10 stand under final rejection, from which this appeal is taken. A copy of the claims on appeal is attached as an Appendix A.

IV Status of Amendments

The independent claims 1 and 10 were amended in response to the Final Office Action of January 27, 2005. In the Response of March 15, 2005 remarks were provided for the allowance of all currently pending claims. There have been no amendments filed subsequent to the March 15th Response. The amendments of the March 15th Response have been entered as denoted in the Advisory Action of April 8, 2005. This Appeal is taken from the state of the claims as amended in the March 15th Response.

V Summary of Claimed Subject Matter

By way of summary, the present invention is directed to a system and method of secured communications. Claims 1 and 10 encompass several points of novelty, and since claims 2-9 depend from claim 1, they also contain at least the same points of novelty as that of claim 1. Independent claims 1 and 10 are similar and are therefore described together.

Claim 1 recites a virtual biological fluid system 10 for secured communications and claim 10 recites a method for secure communications over a network. The system 10 of claim 1 includes a primary gateway that has security information. The system 10 also includes multiple communication layers 22 and a

security control plane 20 that is coupled to and is formed using information from each of the communications layers 22. The security control plane 20 in conjunction with the security information forms a virtual biological fluid 40 that insures secure data transmission. The method of claim 10 has similar limitations as that of the system of claim 1 except security data is generated and utilized to form the virtual biological fluid. The method also includes the formation of a virtual biological fluid where communication between a ground gateway and a station 14 may occur. See page 4, line 9 through page 6, line 10 of the specification.

The system and method of claim 1 and 10 allow for multiple levels of security deployment based on the level of threat. This increases communication protection in the wireless-mobile communication environment where networks are not wired or fixed and topologies of the networks are not fixed and known. The system and method are capable of integrating information from all layers of communication into a secure control plane. See page 6, lines 12-25 of the specification.

Applicant admits that the prior art has included the use of encryption keys for security. Applicant also admits that the prior art has disclosed the use of security managers, which are individual software entities that pre-exist as part of a system. The security managers are used to generate and decode the encryption keys. What is not known or suggested are the several novel limitations recited in claims 1 and 10 and associated aspects thereof, which are utilized in combination. All of the novel limitations of claims 1 and 10 are not taught or suggested by the prior art separately or in combination. The limitations are stated in detail below.

What is not known or suggested is a security control plane that is coupled to and formed using information from each of multiple communication layers. What is also not known or suggested is the formation of a virtual biological fluid via a security control plane and security information to secure data transmission. In addition, what is not known or suggested is the formation of such a virtual biological fluid where communication between a ground gateway and a station may occur.

Claim 2 recites the system of claim 1 and further includes a station 14 in communication with the primary gateway and a satellite 12 in orbit and in communication with the primary gateway and the station 14. The security control plane 20 is on board the satellite 12. See pages 4, lines 9-15, page 5, lines 1-12, and page 6, lines 1-10 of the specification.

Claim 3 recites the system of claim 1 wherein at least one of the communication layers 22 is an application layer 24. See pages 5, lines 2-7 of the specification.

Claim 4 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a presentation layer 26. See pages 5, lines 2-7 of the specification.

Claim 5 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a session layer 28. See pages 5, lines 2-7 of the specification.

Claim 6 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a transport layer 30. See pages 5, lines 2-7 of the specification.

Claim 7 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a network layer 32. See pages 5, lines 2-7 of the specification.

Claim 8 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a data link layer 34. See pages 5, lines 2-7 of the specification.

Claim 9 recites the system of claim 1 wherein at least one of said plurality of communication layers 22 is a physical layer 36. See pages 5, lines 2-7 of the specification.

VI Grounds of Rejection to be Reviewed on Appeal

The following issues are presented in this appeal, which correspond directly to the Examiner's final grounds for rejection in the Final Office Action of January 27, 2005, hereinafter referred to as the "Final Office Action", and in the Advisory Action of April 8, 2005, hereinafter referred to as the "Advisory Action":

(1) whether claims 1 and 10 are patentable under 35 U.S.C. 103(a) over Preston et al. (U.S. Publication No. 2002/0032853) in view of Willis et al. (U.S. Patent No. 6,385,647), and

(2) whether claims 2-9 are patentable under 35 U.S.C. 103(a) over Preston and Willis in view of Greene.

VII Argument

A. THE REJECTION OF CLAIMS 1 and 10 UNDER 35 U.S.C. § 103(a)

Claims 1 and 10 stand fully rejected under 35 U.S.C. § 103(a) over Preston in view of Willis.

Preston discloses a secure dynamic link allocation system for mobile data communication. The system of Preston includes the use of security managers 158 and 178 and multiple communication layers, which are utilized in the sending and receiving of communication signals. The only communication layers that the security managers 158 and 178 are in communication with are the session layers, one of which is identified by numerical designator 152. Link managers exists and/or are disposed between the security managers 158 and 178 and the remaining communication layers, some of which identified by numerical designators 162, 164, and 166. One link manager is identified by numerical designator 159. The security managers 158 and 178 are software entities that pre-exist as part of the system of Preston and are used to generate and decode encryption keys, see paragraphs [0036] and [0044] of Preston. Messages are passed to and from the security managers 158 and 178 in which they are encrypted or decoded.

Willis is directed to a system for selectively routing data via either a network that supports Internet protocol or via a satellite transmission network based on size of the data. The system of Willis includes gateways 800 and 810 having secured information.

Applicant submits that neither Preston nor Willis alone or in combination teach or suggest the limitations of a security control plane coupled to and formed using information from each of multiple communication layers. The Office Actions state that Preston discloses a security control plane formed using information from multiple communication layers. The Office Actions refer to the security managers 158 and 178 of Preston as the security control plane and the passing of messages through different layers of an OSI model using information from each of the layers. Applicant agrees that messages are passed through multiple layers of the OSI model and through the security managers thereof. However, this is irrelevant. Applicant is not claiming the passage of communication messages through multiple communication layers, but rather is claiming the formation of a security control plane. The security control plane claimed is formed from information received from each of the communication layers. The security control plane does not preexist as a software module. The security managers 158 and 178 of Preston are not formed by the communication messages that are passed through the security managers 158 and 178 and communication layers 142, 152, 162, 164, 166, and 170. The security managers 158 and 178 are merely used to provide encryption keying and decoding of the messages. The security managers 158 and 178 do not acquire information from each of the communication layers 142, 152, 162, 164, 166, and 170 and therefrom generate a security control plane, but rather messages are passed in sequence through the communication layers 142, 152, 162, 164, 166, and 170 to the security managers 158 and 178, which encrypt or decode the messages.

Also, security information is not passed from the communication layers 142, 152, 162, 164, 166, and 170 of Preston to the security managers 158 and 178 rather communication messages are passed. Although the messages may be encrypted,

they do not contain security information per se and they clearly do not contain security information, which may be used to form a security device. The claimed system forms the security control plane use security information from the communication layers. For argument sake, since the security managers 158 and 178 preexist and have stored encryption keying techniques, if the security managers 158 and 178 did receive security information from the communication layers 142, 152, 162, 164, 166, and 170 it is not clear what they would do with the information since they are not designed to receive and handle such information. Also, since the security managers 158 and 178 do not receive security information from the communication layers 142, 152, 162, 164, 166, and 170, Preston does not teach or suggest the formation of a security control plane using such information. Nevertheless, nowhere in Preston is the generating, passing, or receiving of security information from the communication layers 142, 152, 162, 164, 166, and 170 mentioned nor is the formation or creation of any item using such information mentioned.

Willis fails to disclose multiple communication layers and thus clearly fails to teach or suggest the formation of a security control plane as claimed.

Also, although Preston may disclose the use of multiple communication layers, Preston only discloses the use of information from a single communication layer, namely the session layer 152. As shown in Figure 1 of Preston, the session layer 152 is coupled to the security manager 158. All other layers of communication are not coupled to nor do they provide information to the security manager 158. In comparing Figure 1 with that of Figure 2 of the present application one can quickly and easily see the difference in the configurations between the system of Preston and that of the present application. The security manager 158 of Preston is in communication with the session layer 152, whereas the system and method of claims 1 and 10 of the present application provide communication between a security plane and multiple communication layers, as is illustrated as an example in Figure 2 of the present application.

The Advisory Action states that the application layer of Preston generates messages that pass through different layers of the OSI model using information from each of the communication layers. Applicant agrees that the application layer 142 generates messages that pass through different layers of the OSI model. However, Applicant submits that Preston does not generate the messages using information from each of the communication layers 142, 152, 162, 164, 166, and 170 and that the passage of the messages between the layers is not in response to security information from each of the layers. The messages of Preston are solely generated in the application layer 142 and are not generated from information collected from each of the communication layers 142, 152, 162, 164, 166, and 170, see paragraph [0035]. Nowhere in Preston is it stated that the application layer 142 contains or provides security information. The session layers of Preston receive the messages and implement or decipher the various protocols. The security managers 158 and 178 encrypt or decode the messages. The other communication layers, specifically the transport layers, the network layers, and the datalink layers, are used simply for networking purposes and have standard networking software, see paragraph [0036] of Preston. Nowhere in Preston is it stated that the security managers 158 and 178 receive information from within the transport layers, the network layers, and the datalink layers or that the stated layers contain security information. The transport layers, the network layers, and the datalink layers are merely used to send and receive the messages over a network.

It is unclear to Applicant how the suggested disclosure by Preston, as stated in the Office Actions and the Advisory Action, of the application layer generating messages that pass through different layers of the OSI model using information from each of the communication layers, discloses the claimed limitations. Applicant does not claim the passage of communication messages between multiple layers, the passage of messages between multiple layers of an OSI model, an OSI model, or the passage of communication messages using information from multiple layers. Applicant claims the generation or formation of a security control plane and a

virtual biological fluid using security information from multiple communication layers. The disclosure stated in the Office Actions and the Advisory Action is directed to the sending and receiving of general communication messages, whereas, the claimed limitations are directed to the generation of security devices. There is a clear and distinct difference between the sending and receiving or passing of general communication messages and the generation of security devices. Also, the mere passage of communication messages between multiple layers does not suggest the use of security information from multiple layers. In fact it appears that none of the layers of Preston provide security information. The only layer of Preston that appears to perhaps use security information, although it is not clear, is the session layer that operates in conjunction with the security managers.

The Final Office Action and the Advisory Action state that the claim language never specifically mentions if the security control plane is specifically coupled to all of the layers of the OSI model. Note that an OSI model is not claimed. Applicant submits that the system and method of claims 1 and 10 recite "a security control plane coupled to and formed using information from each of said plurality of communication layers" and "forming a security control plane using information from each of a plurality of communication layers, said security control plane coupled to said plurality of communication layers", respectively. With respect to claim 1, it is specifically claimed that the security control plane is coupled to each of said plurality of communication layers. With respect to claim 10, it is claimed that the security control plane is formed using information from each of a plurality of communication layers and that the security control plane is coupled to the plurality of communication layers. Thus even the method of claim 10 recites the coupling between the security control plane and the communication layers and the formation thereof using information from all of the communication layers.

In addition, the Final Office Action states that the messages of Preston are transmitted using several widely available communication protocols, such as ACP, WAP, TCP, UDP, SMS, and others. Applicant submits that this is irrelevant. The

claims do not recite the use of communication protocols and the stated protocols have nothing to do with the generation of a security control plane. The communication protocols are merely the sending format that is used in generating the messages in the application layer of Preston. The term "protocol" is defined as a set of rules that define an exact format for communication between systems, see *The American Heritage® Stedman's Medical Dictionary Copyright © 2002, 2001, 1995 by Houghton Mifflin Company.* The term "protocol" does not refer to security information and nowhere in Preston is a security protocol mentioned. The application layers 142 and 170 are not coupled to the security managers 158 and 178 and Preston does not state that the formats utilized contain security information. The security managers 158 and 178 encrypt the messages, regardless of the format, and prior to transmission. The security managers 158 and 178 are not formed from information contained within the messages or as a result of the use of the various protocols.

Furthermore, Preston does not teach or suggest the use of a security control plane, as described above, in conjunction with security information to form a virtual biological fluid. The formation of a virtual biological fluid enables the use of an interactive security doctrine that allows for multiple levels of security deployment. Preston does not teach or suggest such formation and fails to disclose multiple levels of security deployment. The security managers 158 and 178 of Preston exist as single entities between protocol managers and link managers and are coupled to the session layers. The security managers 158 and 178 use a key and encryption for security, see paragraph [0016] and Figures 2A, 2B, and 3 of Preston. The use of a key, as stated in the background section of the present application, does not protect against eavesdropping and data gathering and post processing. The use of a key also does not allow a system to detect a breach in security and may allow for computation sharing for key acquisition. The Office Action states that Preston discloses a system for layered and secured data communication. Applicant submits

that the key and encryption of Preston are utilized in a single layer, or in the session layers.

Moreover, with respect to claim 10, nowhere in Preston or in Willis is the generation of a virtual biological fluid or the like generated or formed using a security control plane in conjunction with security data, whereby secure data transmission between a ground gateway and a station may occur. The Office Actions have admitted that Preston fails to disclose a gateway and as stated above neither reference teaches or suggests the formation of a virtual biological fluid. Thus, clearly the formation of a virtual biological fluid where secure data transmission between a ground gateway and a station may occur is also not disclosed by either reference alone or in combination.

Referring to MPEP § 2143.01, the fact that references can be combined or modified is not sufficient to establish *prima facie* obviousness. The prior art must also suggest the desirability of the combination and the modification, *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). None of the references suggest such combination and clearly none of the references suggest performing some sort of combination and modification thereof to arrive at the system and method of claims 1 and 10.

Referring to MPEP 2141.01(a), while the Patent Office classification of references and cross-references in the official search notes are some evidence of "nonanalogy" or "analogy" respectively, the court has found "the similarities and differences in structure and function of the inventions to carry far greater weight." *In re Ellis*, 476 F.2d 1370, 1372, 177USPQ526, 527 (CCPA 1973). Willis would not have logically commended itself to an inventor's attention in considering the problems solved by the system and method of claims 1 and 10. In developing a satellite system for secured communication, one would clearly not look to a method for selectively routing data based on the size of the data. Willis is directed to the efficiency of data communication not the security thereof. Although Willis mentions that a secure transfer protocol may be used, Willis does not describe the

operation, functioning, or configuration of a security system. The system of Willis would not have logically commended itself to the Applicant's attention in solving the problems associated with secure communication. Willis would not be reasonably pertinent to the particular problems solved by the system and method of claims 1 and 10. Thus, Willis is nonanalogous art.

Since Preston and Willis alone or in combination fail to teach or suggest each and every limitation of claims 1 and 10, Applicant submits that the *prima facie* case of obviousness has not been met. See MPEP 706.02(j) and 2143, which states that to establish a *prima facie* case of obviousness the prior art reference(s) must teach or suggest all the claim limitations. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Thus, Applicant submits that claims 1 and 10 are believed to be independently patentable and allowable for the reasons set forth above.

B. THE REJECTION OF CLAIMS 2-9 UNDER 35 U.S.C. § 103(a)

Claims 2-9 stand fully rejected as being unpatentable under 35 U.S.C. 103(a) over Preston and Willis in view of Greene.

Applicant submits that since claims 2-9 depend from claim 10 that they are also independently patentable and allowable for at least the same reasons.

Claim 2 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites a station 14 in communication with the primary gateway and a satellite 12 in orbit and in communication with the primary gateway and the station 14. The security control plane 20 is on board the satellite 12. The Non-Final Office Action states that Preston and Willis fail to disclose a security control plane onboard a satellite. Applicant agrees. However, Applicant submits that Greene also fails to disclose a security control plane, and especially a security control plane as claimed.

Greene discloses a secure keypad implementation or pin blocks in which encrypted keys are entered to allow for communication between secured keypads

10 and 11. The keypads 10 and 11 are operated under the domain of a single processing board 12. Once the secure keypads 10 and 11 receive the encrypted codes they indicate that they have control of the transaction. Once an exchange session is completed messages are passed between the keypads 10 and 11. The messages are encrypted, like in Preston, and decrypted by the receiving keypad. Again the encryption and decryption of keys is not the same as a security control plane or the formation of a security control plane. Encryption refers to the translation of data into a secret code. Encryption codes are previously stored and utilized; they are not formed during operation. A security control plane contains security information and is an interactive entity, which is formed during operation. The keypads 10 and 11 are also not formed during operation and do not form interactive entities. The keypads 10 and 11 are not security control planes, but are rather data entry devices. Surely, the encryption and the keypads described in Greene are not the same as a security control plane that is formed in response to security information received from multiple communication layers. Greene does not even disclose multiple communication layers. Thus, claim 2 is further novel and nonobvious for the above stated reasons over that of claim 1.

Claim 3 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of the communication layers 22 is an application layer 24.

Claim 4 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a presentation layer 26.

Claim 5 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a session layer 28.

Claim 6 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a transport layer 30.

Claim 7 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a network layer 32.

Claim 8 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a data link layer 34.

Claim 9 is believed to be independently patentable and allowable for the reasons set forth above since it depends from claim 1 and further recites wherein at least one of said plurality of communication layers 22 is a physical layer 36.

VIII Appendix

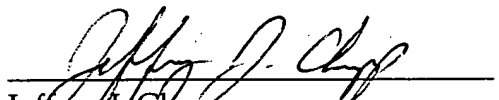
A copy of the claims involved in this Appeal, namely claims 1-10, is attached hereto as Appendix A.

IX Conclusion

For the reasons advanced above, Appellant respectfully contends that each claim is patentable. Therefore reversal of the rejection is requested.

Respectfully submitted,

ARTZ & ARTZ, P.C.

By: 

Jeffrey J. Chapp
Registration No. 50,579
28333 Telegraph Road, Suite 250
Southfield, MI 48034
(248) 223-9500

Dated: May 20, 2005

APPENDIX A

What is claimed is:

1. A virtual biological fluid system for secure communications, said system comprising:

a primary gateway having security information;

a plurality of communication layers, and

a security control plane coupled to and formed using information from each of said plurality of communications layers, whereby said security control plane in conjunction with said security information forms a virtual biological fluid insuring secure data transmission.

2. The system as recited in claim 1, further comprising:

at least one station in communication with said primary gateway; and

a satellite in orbit and in communication with said primary gateway and said at least one station, and said security control plane is on board said satellite.

3. The system as recited in claim 1, wherein at least one of said plurality of communication layers is an application layer.

4. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a presentation layer.

5. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a session layer.

6. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a transport layer.

7. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a network layer.

8. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a data link layer.

9. The system as recited in claim 1, wherein at least one of said plurality of communication layers is a physical layer.

10. A method for secure communications over a network, said method comprising the steps of:

generating security data;

forming a security control plane using information from each of a plurality of communication layers, said security control plane coupled to said plurality of communication layers;

forming a virtual biological fluid using said security control plane in conjunction with said security data, whereby secure data transmission between a ground gateway and a station may occur; and

communicating secure data between said ground gateway and said station.